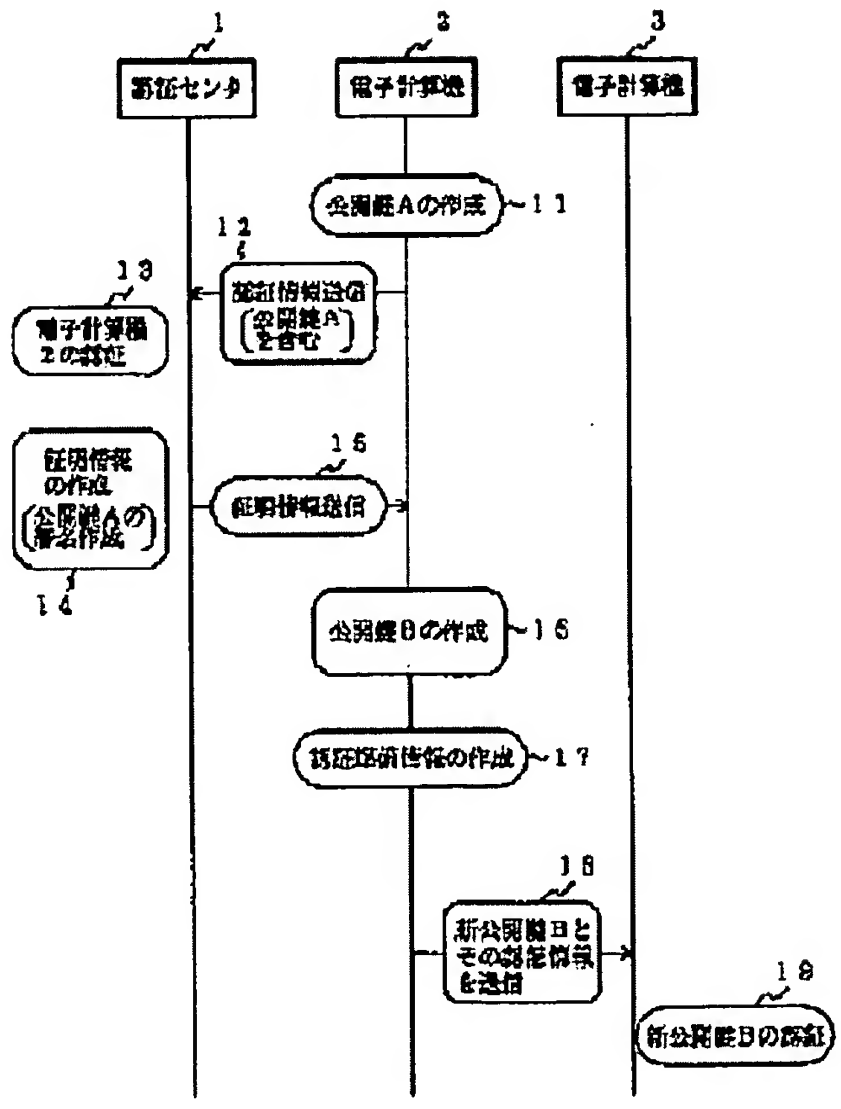
VERIFICATION METHOD FOR COMPUTER SYSTEM

Publication number: JP9261218
Publication date: 1997-10-03
Inventor: HAYASHI SEIICHIRO
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
- international: ***G09C1/00; H04L9/32;*** **G09C1/00; H04L9/32;** (IPC1-7): H04L9/32; G09C1/00
- european:
Application number: JP19960072035 19960327
Priority number(s): JP19960072035 19960327

Abstract of **JP9261218**

PROBLEM TO BE SOLVED: To allow a system to attain verification of new verification information generated by a computer without acquisition of certificate information from a verification center. SOLUTION: A computer 2 generates at first a public key A (11), and sends verification information including the public key to a verification center 1 (12). The verification center 1 confirms the public key A to be a key of the computer 2 based on the verification information (13), generates digital signature information (verification information) of the public key A (14) and returns the information to the computer 2 (15). The computer 2 generates newly the public key B (16) and generates verification preparation information by adding the signature information of the public key A to the public key B (17), the verification preparation information is ciphered by a secret key A and the resulting information is sent to a computer 3 (18). The computer 3 decodes the received information the public key A to verify the public key B is the computer 2 it self based on the signature information in the decoded information.



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the informational authentication approach of guaranteeing the communications partner in the computing system to which the computer (authentication center) which has the authority function which authorizes two or more computer and each computer was connected in the network, and in detail, when a computer newly creates authentication information, it relates to the approach of attesting again, without acquiring certification information from an authentication center.
[0002]
[Description of the Prior Art] When it set to the system which performs a digital signature communication link and a certain computer added and changed a public key by the public key cryptosystem conventionally, certification information, such as a digital signature, was newly got from the authentication center to the public key added and changed. That is, the authentication center was generating the certification information (equivalent to a certified seal registration) on a public key belonging to him by the digital signature of an authentication center each time.
[0003]
[Problem(s) to be Solved by the Invention] By the conventional approach, whenever a computer adds and changes a public key etc., it will connect with an authentication center and a digital signature will be generated. That is, since the digital signature of the past which the authentication center generated was not conventionally used effectively for authentication of other public keys etc., whenever the computer created a new public key etc., it needed to be requested from the authentication center, needed to receive the digital signature, and had the problem on which the burden and traffic of the computer which receives an authentication center and authentication increase.
[0004] The purpose of this invention tends to give the same guarantee as having been attested from this authentication center, without minding an authentication center about authentication information, such as a new public key, based on the certification information which is the fact once attested by the authentication center.
[0005]
[Means for Solving the Problem] The authentication approach of this invention uses the certification information once attested by the authentication center. A certain computer 2 adds the certification information attested by this authentication center to the newly created authentication information, and it transmits to other computers 3. a radical [information / which is added to the new authentication information received with these other computers 3 / certification] -- this -- it is having enabled it to attest that new authentication information is the thing of a computer 2.
[0006] A computer 2 presupposes that the public key A with a digital signature of an authentication center is held as certification already attested from the authentication center. the whole of the information this computer 2 indicates [the public key A with a digital signature of an authentication center and the public key B newly added or changed, and] it to be whether a public key B is

modification or an addition further -- the private key A of a public key A -- encryption -- or a digital signature is carried out and it transmits to other computers 3. The public key B which is informational contents a decryption or by carrying out a digital signature about the this received information can attest that it is computer 2 his public key as well as a public key A with a public key A from encryption or the digital signature being carried out with the private key A corresponding to the public key A with which the received information was guaranteed from the authentication center in the computer 3.

[0007]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained using a drawing. Drawing 1 is what showed the block diagram of the target system by this invention, and two or more computers 2, 3, and 4 are connected with the authentication center 1 by the channel (network) 5. Here, each computers 2, 3, and 4 presuppose that a digital signature communication link is performed by the public key cryptosystem.

[0008] Drawing 2 shows the authentication procedure of the public key by this invention. Here, it shall attest that a computer 3 is the thing of this computer 2 about the public key which a computer 1 newly changes and adds.

[0009] <Example 1> A computer 2 this The public key A with a digital signature of the authentication center 1 The public key B newly added or changed and this public key B make information which shows modification or an addition authentication preparation information. It is the example which this authentication preparation information is enciphered with the private key A of a public key A, it transmits to a computer 3, and a computer 3 decodes the this enciphered authentication preparation information with a public key A, and attests a public key B with it being the thing of a computer 2. Hereafter, this example is explained based on drawing 2 .

[0010] Step 1: The authentication computer 2 of the public key A by the authentication center transmits authentication information to the authentication center 1 by processing 12 about public key A <KpA> created by processing 11. Here, the information <ID> which guarantees the identity of a computer 2 other than public key A <KpA> is included in the authentication information transmitted to the authentication center 1 by processing 12. Surely in the authentication center 1, it checks that a public key A belongs to computer 2 him by processing 13 based on the authentication information transmitted by processing 12. To the information <KpA|TIME|ID> which combined the term information <TIME> which the authentication information <ID> and the authentication center 1 of public key A <KpA> and a computer 2 moreover give at processing 14, a digital signature is carried out with the private key <KsCA> of this authentication center 1, signature information <SKsCA (KpA|TIME|ID)> is generated, and it transmits to a computer 2 by processing 15.

SY (XXX): Digital signature a|b to XXX of a private key Y : a and b are connected.

[0011] Step 2: The creation computer 2 of the information which guarantees the new public key B creates public key B <KpB> by processing 16, and a public key B creates further the flag information which shows an addition or modification. In processing 17, authentication information <ID> is combined with the information created by processing 16, the digital signature <SKsCA (KpA|TIME|ID) > by the authentication center 1 of the public key A further generated at step 11 is added, and authentication preparation information <KpB|ID, SKsCA (KpA|TIME|ID)> is created. To this authentication preparation information, it enciphers by private key [of a public key A] A <KsA>, and a computer 2 transmits encryption information <EKsA (KpB|ID, SKsCA (KpA|TIME|ID))> to a computer 3 by processing 18.

EY (XXX): Encipher XXX with a private key Y.

[0012] Step 3: Decrypt the encryption information transmitted by the computer 2 by processing 18 by processing 19 at public key [of a computer 2] A <KpA> in the authentication computer 3 by the other computers of the new public key B. Namely, <DKpA(EKsA (KpB|ID, SKsCA (KpA|TIME|ID))) =KpB|ID, SKsCA (KpA|TIME|ID). When signature verification of the digital signature <SKsCA (KpA|TIME|ID)> of the authentication center 1 to a public key A is carried out with the public key <KpCA> of the authentication center 1 among the decrypted information, verification passes and authentication information <ID> is further in agreement with a computer 2, a public key B attests as a

public key of a computer 2.
DY (XXX): Decrypt XXX with a public key Y.
[0013] <Example 2> A computer 2 this The public key A with a digital signature of the authentication center 1 The public key B newly added or changed and this public key B make information which shows modification or an addition authentication preparation information. It is the example which the signature information which carried out the digital signature of this authentication preparation information with the private key A is transmitted to a computer 3 with authentication preparation information, and a computer 3 verifies the digital signature of authentication preparation information with the public key A of a computer 2, and attests a public key B with it being the thing of a computer 2.
[0014] authentication of the public key A by the Step 1:authentication center -- this is the same as that of an example 1.
[0015] Step 2: It is the same as that of an example 1 till the place where the creation computer 2 of the information which guarantees a new public key creates authentication preparation information by processing 17. A computer 2 transmits the signature information <SKsA (KpB|ID, SKsCA (KpA|TIME|ID))> and authentication preparation information <KpB|ID, SKsCA (KpA|TIME|ID)> which carried out the digital signature of the created authentication preparation information <KpB|ID, SKsCA (KpA|TIME|ID)> by private key A <KsA> to a computer 3 by processing 18.
[0016] Step 3: Verify the digital signature <SKsA (KpB|ID, SKsCA (KpA|TIME|ID))> of the authentication preparation information transmitted from the computer 2 by processing 18 by processing 19 in the authentication computer 3 by the other computers of a new public key at public key [of a computer 2] A <KpA>. Furthermore, when signature verification of the digital signature <SKsCA (KpA|TIME|ID)> of the authentication center 1 to a public key A is carried out with the public key <KpCA> of the authentication center 1, verification passes and authentication information <ID> is further in agreement with a computer 2, public key B <KpB> attests as a public key of a computer 2.
[0017]
[Effect of the Invention] As explained above, once it receives the authentication from an authentication center according to the authentication approach of this invention, the guarantee of a new public key will be attained without receiving modification of a subsequent public key and authentication of a public key new from an authentication center at every addition. For this reason, the burden of the computer which creates an authentication center and a new public key and receives authentication, and the burden of traffic are mitigated.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In the authentication approach of a computing system that the computer (henceforth an authentication center) which has the authority function which authorizes two or more computer and each computer was connected in the network A certain computer adds the certification information which guarantees what was attested by the authentication center, and the new authentication information which the computer concerned created is transmitted to other computers. In other computers a radical [information / which is added to the new authentication information on said received computer / certification] -- this -- the authentication approach of the computing system characterized by new authentication information attesting with the thing of said computer.
[Claim 2] In the authentication approach of a computing system according to claim 1 each computer by the public key cryptosystem The public key A with a digital signature with which it is the system equipped with the verification function of generation of a digital signature, and a signature, and the digital signature of a certain computer was carried out by the authentication center A different public key B from said public key A and said public key B make identification information from which modification of a public key A discriminates whether it is an addition authentication preparation information. Said authentication preparation information is enciphered with the private key A corresponding to a public key A, and the this enciphered authentication preparation information is transmitted to other computers. A computer besides the above The authentication approach of the computing system which decodes said received authentication preparation information which was enciphered with a public key A, and is characterized by attesting with it being the public key of said computer with which the authentication center attested said public key B based on the this decoded authentication preparation information.
[Claim 3] In the authentication approach of a computing system according to claim 1 each computer by the public key cryptosystem The public key A with a digital signature with which it is the system equipped with the verification function of generation of a digital signature, and a signature, and the digital signature of a certain computer was carried out by the authentication center A different public key B from said public key A and said public key B make identification information from which modification of a public key A discriminates whether it is an addition authentication preparation information. The signature information and authentication preparation information which carried out the digital signature of this authentication preparation information with the private key A are transmitted to other computers. A computer besides the above The authentication approach of the computing system characterized by attesting with it being the public key of said computer with which the signature information on said received authentication preparation information was verified with the public key A, and the authentication center attested said public key B.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（A）　(11)特許出願公開番号

特開平9－261218

(43)公開日　平成９年(1997)10月３日

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI		技術表示箇所
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７５Ｂ
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ｂ

審査請求　未請求　請求項の数３　ＯＬ　（全　４　頁）

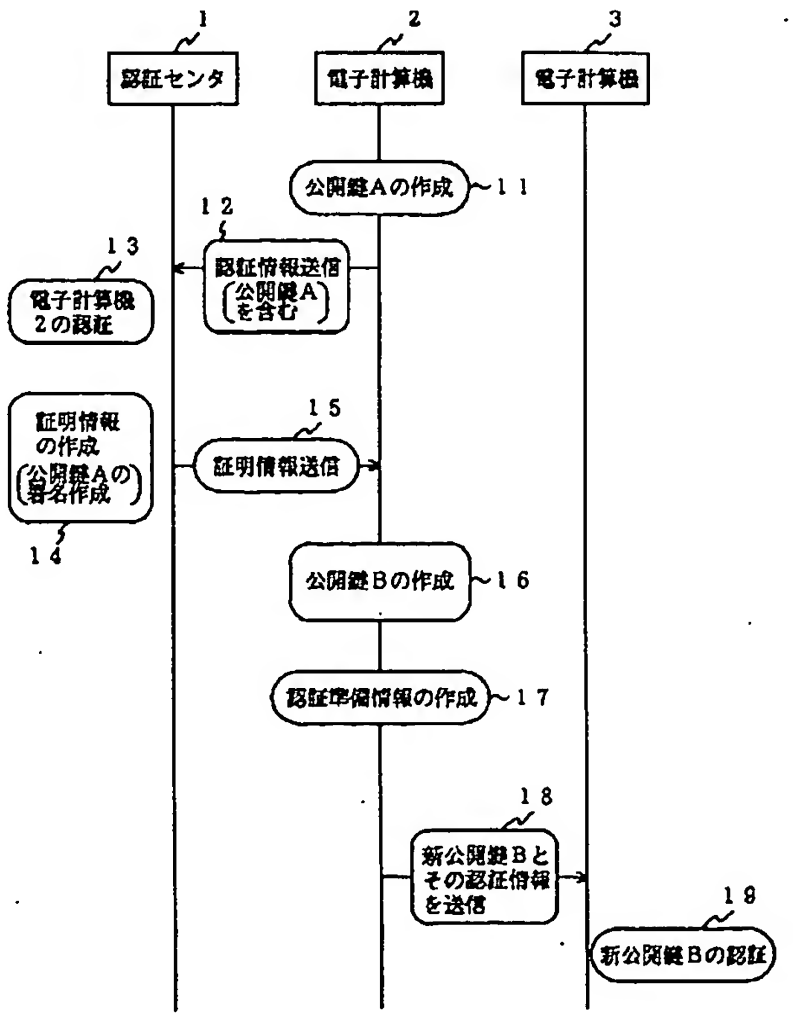
(21)出願番号　特願平8－72035

(22)出願日　平成８年(1996)３月27日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(72)発明者　林　誠一郎
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　弁理士　鈴木　誠

(54)【発明の名称】　計算機システムの認証方法

(57)【要約】
【課題】　計算機が作成する新たな認証情報について、認証センタから証明情報を得ることなく認証を可能とする。
【解決手段】　計算機２は、最初に公開鍵Ａを作成すると（１１）、該公開鍵Ａを含む認証情報を認証センタ１に送信する（１２）。認証センタ１では、認証情報を基に公開鍵Ａが計算機２のものであることを確認し（１３）、該公開鍵Ａのディジタル署名情報（証明情報）を生成し（１４）、計算機２に返送する（１５）。計算機２は、新たに公開鍵Ｂを作成すると（１６）、該公開鍵Ｂに公開鍵Ａの署名情報を加えて認証準備情報を作成し（１７）、該認証準備情報を秘密鍵Ａで暗号化して計算機３に送信する（１８）。計算機３では、受信した情報を公開鍵Ａで復号し、該復号化した情報中の署名情報を基に公開鍵Ｂが計算機２本人のものと認証する（１９）。



【特許請求の範囲】
【請求項１】　複数の電子計算機と各電子計算機を認定するオーソリティ機能を有する電子計算機（以下、認証センタという）とがネットワークで接続された計算機システムの認証方法において、
ある電子計算機が、認証センタにより認証されたことを保証する証明情報を付加して、当該電子計算機が作成した新たな認証情報を他の電子計算機へ送信し、
他の電子計算機では、受信した前記電子計算機の新たな認証情報に付加されている証明情報を基に、該新たな認証情報が前記電子計算機のものと認証することを特徴とする計算機システムの認証方法。
【請求項２】　請求項１記載の計算機システムの認証方法において、各電子計算機が公開鍵暗号方式により、ディジタル署名の生成と署名の検証機能を備えたシステムであって、
ある電子計算機が、認証センタによりディジタル署名されたディジタル署名付き公開鍵Ａと、前記公開鍵Ａとは異なる公開鍵Ｂと、前記公開鍵Ｂが公開鍵Ａの変更が追加かを識別する識別情報とを認証準備情報として、公開鍵Ａに対応する秘密鍵Ａで前記認証準備情報を暗号化し、該暗号化した認証準備情報を他の電子計算機に送信し、
前記他の電子計算機は、受信した前記暗号化された認証準備情報を公開鍵Ａで復号し、該復号した認証準備情報を基に、前記公開鍵Ｂを、認証センタが認証した前記電子計算機の公開鍵であると認証することを特徴とする計算機システムの認証方法。
【請求項３】　請求項１記載の計算機システムの認証方法において、各電子計算機が公開鍵暗号方式により、ディジタル署名の生成と署名の検証機能を備えたシステムであって、
ある電子計算機が、認証センタによりディジタル署名されたディジタル署名付き公開鍵Ａと、前記公開鍵Ａとは異なる公開鍵Ｂと、前記公開鍵Ｂが公開鍵Ａの変更が追加かを識別する識別情報とを認証準備情報として、該認証準備情報を秘密鍵Ａでディジタル署名した署名情報と認証準備情報とを他の電子計算機に送信し、
前記他の電子計算機は、受信した前記認証準備情報の署名情報を公開鍵Ａで検証し、前記公開鍵Ｂを、認証センタが認証した前記電子計算機の公開鍵であると認証することを特徴とする計算機システムの認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、複数の電子計算機と各電子計算機を認定するオーソリティ機能を有する電子計算機（認証センタ）がネットワークで接続された計算機システムにおける通信相手を保証する情報の認証方法に係り、詳しくは、電子計算機が認証情報を新たに作成した場合、再度、認証センタから証明情報を得ることなく認証する方法に関する。
【０００２】
【従来の技術】従来、公開鍵暗号方式でディジタル署名通信を行うシステムにおいて、ある電子計算機が公開鍵を追加・変更する場合には、認証センタから追加・変更する公開鍵に対して、新たにディジタル署名等の証明情報をもらっていた。すなわち、認証センタのディジタル署名により、公開鍵が本人のものであることの証明情報（印鑑証明に相当）を、認証センタがその都度生成していた。
【０００３】
【発明が解決しようとする課題】従来の方法では、電子計算機が公開鍵等を追加・変更する都度、認証センタに接続してディジタル署名を生成することになってしまう。すなわち、従来は認証センタが生成した過去のディジタル署名が他の公開鍵等の認証に有効利用されていないため、電子計算機は新たな公開鍵等を作成する都度、認証センタに依頼してディジタル署名を受ける必要があり、認証センタと認証を受ける電子計算機の負担及び通信量が増大する問題があった。
【０００４】本発明の目的は、一度認証センタによって認証された事実である証明情報を基に、新たな公開鍵等の認証情報について、認証センタを介さずに該認証センタから認証されたと同様の保証を与えようとするものである。
【０００５】
【課題を解決するための手段】本発明の認証方法は、一度認証センタによって認証された証明情報を使い、ある電子計算機２が、新たに作成した認証情報に該認証センタによって認証された証明情報を付加して他の電子計算機３に送信し、該他の電子計算機３にて、受信した新たな認証情報に付加されている証明情報を基に、該新たな認証情報が電子計算機２のものであることを認証できるようにしたことである。
【０００６】電子計算機２は、認証センタからすでに認証された証明として認証センタのディジタル署名付き公開鍵Ａを保有しているとする。該電子計算機２は、認証センタのディジタル署名付き公開鍵Ａおよび新たに追加もしくは変更する公開鍵Ｂ、さらに公開鍵Ｂが変更か追加なのか示す情報の全体を、公開鍵Ａの秘密鍵Ａで暗号化もしくはディジタル署名し、他の電子計算機３に送信する。電子計算機３では、受信した情報が、認証センタから保証された公開鍵Ａに対応する秘密鍵Ａで暗号化もしくはディジタル署名されていることから、該受信した情報を公開鍵Ａで復号化もしくはディジタル署名することにより、情報の中身である公開鍵Ｂも公開鍵Ａと同様に電子計算機２本人の公開鍵であることが認証できる。
【０００７】
【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図１は、本発明で対象とする

システムのブロック図を示したもので、認証センタ１と複数の電子計算機２，３，４が通信路（ネットワーク）５で接続されている。ここで、各電子計算機２，３，４は公開鍵暗号方式でディジタル署名通信を行うとする。

【０００８】図２は、本発明による公開鍵の認証手順を示したものである。ここでは、電子計算機１が新たに変更・追加する公開鍵を、電子計算機３が該電子計算機２のものであることを認証するものとする。

【０００９】〈実施例１〉これは、電子計算機２が、認証センタ１のディジタル署名付き公開鍵Ａと、新たに追加もしくは変更する公開鍵Ｂと、該公開鍵Ｂが変更か追加かを示す情報とを認証準備情報として、該認証準備情報を公開鍵Ａの秘密鍵Ａで暗号化して電子計算機３に送信し、電子計算機３が、該暗号化された認証準備情報を公開鍵Ａで復号し、公開鍵Ｂを電子計算機２のものであると認証する実施例である。以下、本実施例を図２に基づいて説明する。

【００１０】ステップ１：認証センタによる公開鍵Ａの認証

電子計算機２は、処理１１により作成した公開鍵Ａ〈ＫｐＡ〉について、処理１２により認証情報を認証センタ１に送信する。ここで、処理１２で認証センタ１に送信される認証情報には、公開鍵Ａ〈ＫｐＡ〉の他に電子計算機２の身元を保証する情報〈ＩＤ〉を含む。認証センタ１では、処理１２で送信された認証情報を基に、処理１３にて確かに公開鍵Ａは電子計算機２本人のものであることを確認する。その上で、処理１４にて公開鍵Ａ〈ＫｐＡ〉と電子計算機２の認証情報〈ＩＤ〉と認証センタ１が付与する期限情報〈ＴＩＭＥ〉等を結合した情報〈ＫｐＡ｜ＴＩＭＥ｜ＩＤ〉に対して、該認証センタ１の秘密鍵〈ＫｓＣＡ〉でディジタル署名して、署名情報〈ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を生成し、処理１５により電子計算機２に送信する。

ＳＹ（ＸＸＸ）：秘密鍵ＹのＸＸＸに対するディジタル署名

ａ｜ｂ　　：ａとｂを連結。

【００１１】ステップ２：新たな公開鍵Ｂを保証する情報の作成

電子計算機２が、処理１６により公開鍵Ｂ〈ＫｐＢ〉を作成し、さらに公開鍵Ｂが追加か変更かを示すフラグ情報を作成する。処理１７では、処理１６で作成した情報に認証情報〈ＩＤ〉を結合し、さらにステップ１１で生成した公開鍵Ａの認証センタ１によるディジタル署名〈ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を加えて認証準備情報〈ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を作成する。電子計算機２は、この認証準備情報に対して、公開鍵Ａの秘密鍵Ａ〈ＫｓＡ〉で暗号化し、暗号化情報〈ＥＫｓＡ（ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ））〉を処理１８により電子計算機３に送信する。

ＥＹ（ＸＸＸ）：秘密鍵ＹでＸＸＸを暗号化。

【００１２】ステップ３：新たな公開鍵Ｂの他電子計算機による認証

電子計算機３では、処理１９により、処理１８で電子計算機２により送信された暗号化情報を電子計算機２の公開鍵Ａ〈ＫｐＡ〉で復号化する。即ち、〈ＤＫｐＡ（ＥＫｓＡ（ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ））＝ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）。復号化した情報のうち、公開鍵Ａに対する認証センタ１のディジタル署名〈ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を認証センタ１の公開鍵〈ＫｐＣＡ〉で署名検証し、検証が合格し、さらに認証情報〈ＩＤ〉が電子計算機２と一致した場合に、公開鍵Ｂが電子計算機２の公開鍵として認証する。

ＤＹ（ＸＸＸ）：公開鍵ＹでＸＸＸを復号化。

【００１３】〈実施例２〉これは、電子計算機２が、認証センタ１のディジタル署名付き公開鍵Ａと、新たに追加もしくは変更する公開鍵Ｂと、該公開鍵Ｂが変更か追加かを示す情報とを認証準備情報とし、該認証準備情報を秘密鍵Ａでディジタル署名した署名情報を認証準備情報とともに電子計算機３に送信し、電子計算機３が、認証準備情報のディジタル署名を電子計算機２の公開鍵Ａで検証し、公開鍵Ｂを電子計算機２のものであると認証する実施例である。

【００１４】ステップ１：認証センタによる公開鍵Ａの認証

これは実施例１と同様である。

【００１５】ステップ２：新たな公開鍵を保証する情報の作成

電子計算機２が処理１７にて認証準備情報を作成するところまでは実施例１と同様である。電子計算機２は、作成した認証準備情報〈ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を秘密鍵Ａ〈ＫｓＡ〉でディジタル署名した署名情報〈ＳＫｓＡ（ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ））〉と認証準備情報〈ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を、処理１８により電子計算機３に送信する。

【００１６】ステップ３：新たな公開鍵の他電子計算機による認証

電子計算機３では、処理１９により、処理１８で電子計算機２より送信された認証準備情報のディジタル署名〈ＳＫｓＡ（ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ））〉を電子計算機２の公開鍵Ａ〈ＫｐＡ〉で検証する。さらに、公開鍵Ａに対する認証センタ１のディジタル署名〈ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を認証センタ１の公開鍵〈ＫｐＣＡ〉で署名検証し、検証が合格し、さらに認証情報〈ＩＤ〉が電子計算機２と一致した場合に、公開鍵Ｂ〈ＫｐＢ〉が電子計算機２の公開鍵として認証する。

【００１７】

システムのブロック図を示したもので、認証センタ１と複数の電子計算機２，３，４が通信路（ネットワーク）５で接続されている。ここで、各電子計算機２，３，４は公開鍵暗号方式でディジタル署名通信を行うとする。

【０００８】図２は、本発明による公開鍵の認証手順を示したものである。ここでは、電子計算機１が新たに変更・追加する公開鍵を、電子計算機３が該電子計算機２のものであることを認証するものとする。

【０００９】〈実施例１〉これは、電子計算機２が、認証センタ１のディジタル署名付き公開鍵Ａと、新たに追加もしくは変更する公開鍵Ｂと、該公開鍵Ｂが変更か追加かを示す情報とを認証準備情報として、該認証準備情報を公開鍵Ａの秘密鍵Ａで暗号化して電子計算機３に送信し、電子計算機３が、該暗号化された認証準備情報を公開鍵Ａで復号し、公開鍵Ｂを電子計算機２のものであると認証する実施例である。以下、本実施例を図２に基づいて説明する。

【００１０】ステップ１：認証センタによる公開鍵Ａの認証

電子計算機２は、処理１１により作成した公開鍵Ａ〈ＫｐＡ〉について、処理１２により認証情報を認証センタ１に送信する。ここで、処理１２で認証センタ１に送信される認証情報には、公開鍵Ａ〈ＫｐＡ〉の他に電子計算機２の身元を保証する情報〈ＩＤ〉を含む。認証センタ１では、処理１２で送信された認証情報を基に、処理１３にて確かに公開鍵Ａは電子計算機２本人のものであることを確認する。その上で、処理１４にて公開鍵Ａ〈ＫｐＡ〉と電子計算機２の認証情報〈ＩＤ〉と認証センタ１が付与する期限情報〈ＴＩＭＥ〉等を結合した情報〈ＫｐＡ｜ＴＩＭＥ｜ＩＤ〉に対して、該認証センタ１の秘密鍵〈ＫｓＣＡ〉でディジタル署名して、署名情報〈ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を生成し、処理１５により電子計算機２に送信する。

ＳＹ（ＸＸＸ）：秘密鍵ＹのＸＸＸに対するディジタル署名

ａ｜ｂ　　：ａとｂを連結。

【００１１】ステップ２：新たな公開鍵Ｂを保証する情報の作成

電子計算機２が、処理１６により公開鍵Ｂ〈ＫｐＢ〉を作成し、さらに公開鍵Ｂが追加か変更かを示すフラグ情報を作成する。処理１７では、処理１６で作成した情報に認証情報〈ＩＤ〉を結合し、さらにステップ１１で生成した公開鍵Ａの認証センタ１によるディジタル署名〈ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を加えて認証準備情報〈ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を作成する。電子計算機２は、この認証準備情報に対して、公開鍵Ａの秘密鍵Ａ〈ＫｓＡ〉で暗号化し、暗号化情報〈ＥＫｓＡ（ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ））〉を処理１８により電子計算機３に送信する。

ＥＹ（ＸＸＸ）：秘密鍵ＹでＸＸＸを暗号化。

【００１２】ステップ３：新たな公開鍵Ｂの他電子計算機による認証

電子計算機３では、処理１９により、処理１８で電子計算機２により送信された暗号化情報を電子計算機２の公開鍵Ａ〈ＫｐＡ〉で復号化する。即ち、〈ＤＫｐＡ（ＥＫｓＡ（ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ））＝ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）。復号化した情報のうち、公開鍵Ａに対する認証センタ１のディジタル署名〈ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を認証センタ１の公開鍵〈ＫｐＣＡ〉で署名検証し、検証が合格し、さらに認証情報〈ＩＤ〉が電子計算機２と一致した場合に、公開鍵Ｂが電子計算機２の公開鍵として認証する。

ＤＹ（ＸＸＸ）：公開鍵ＹでＸＸＸを復号化。

【００１３】〈実施例２〉これは、電子計算機２が、認証センタ１のディジタル署名付き公開鍵Ａと、新たに追加もしくは変更する公開鍵Ｂと、該公開鍵Ｂが変更か追加かを示す情報とを認証準備情報とし、該認証準備情報を秘密鍵Ａでディジタル署名した署名情報を認証準備情報とともに電子計算機３に送信し、電子計算機３が、認証準備情報のディジタル署名を電子計算機２の公開鍵Ａで検証し、公開鍵Ｂを電子計算機２のものであると認証する実施例である。

【００１４】ステップ１：認証センタによる公開鍵Ａの認証

これは実施例１と同様である。

【００１５】ステップ２：新たな公開鍵を保証する情報の作成

電子計算機２が処理１７にて認証準備情報を作成するところまでは実施例１と同様である。電子計算機２は、作成した認証準備情報〈ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を秘密鍵Ａ〈ＫｓＡ〉でディジタル署名した署名情報〈ＳＫｓＡ（ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ））〉と認証準備情報〈ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を、処理１８により電子計算機３に送信する。

【００１６】ステップ３：新たな公開鍵の他電子計算機による認証

電子計算機３では、処理１９により、処理１８で電子計算機２より送信された認証準備情報のディジタル署名〈ＳＫｓＡ（ＫｐＢ｜ＩＤ，ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ））〉を電子計算機２の公開鍵Ａ〈ＫｐＡ〉で検証する。さらに、公開鍵Ａに対する認証センタ１のディジタル署名〈ＳＫｓＣＡ（ＫｐＡ｜ＴＩＭＥ｜ＩＤ）〉を認証センタ１の公開鍵〈ＫｐＣＡ〉で署名検証し、検証が合格し、さらに認証情報〈ＩＤ〉が電子計算機２と一致した場合に、公開鍵Ｂ〈ＫｐＢ〉が電子計算機２の公開鍵として認証する。

【００１７】